U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Automated Access Control and Computer Enhanced Security System (ACCESS)

Date: September 3, 2021

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system: (*Use plain language, no technical terms.*)

The Automated Access Control and Computer Enhanced Security System Federal Information Security Management Act (ACCESS FISMA) boundary includes systems that ensure the physical safety and security of agency facilities. The systems operate under U.S. Nuclear Regulatory Commission (NRC) Privacy Act systems of records NRC-39, "Personnel Security Files and Associated Records," NRC-40, "Facility Security Access Controls Records," and NRC-45, "Digital Certificates for Personal Identity Verification Records."

The ACCESS FISMA boundary has the following system components:

- Physical Access Control System (PACS)
- Closed-Circuit Television (CCTV) System
- Intrusion Detection System (IDS)
- Radio Communications System (RCS)
- Building Management System (BMS) – Heating, Ventilation, & Air Conditioning (HVAC) and Lighting
- Some peripherals used by the NRC when issuing Personal Identity Verification (PIV) cards are also within the ACCESS FISMA boundary.

2. What agency function does it support? (*How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)*)

The systems in the ACCESS FISMA boundary are support-systems and do not directly drive the agency mission. They ensure the physical safety and security of personnel, property, information, infrastructure, and assets.

3. Describe any modules or subsystems, where relevant, and their functions.

The ACCESS FISMA boundary has the following system components and some equipment used by the NRC when issuing PIV cards.

1. **Physical Access Control System**: The NRC uses the PACS system to control access to the NRC campuses and buildings.

2. **Closed-Circuit Television System**: NRC emergency-response personnel use the closed-circuit TV system, comprised of digital surveillance cameras, to monitor the headquarter campus and buildings.

3. **Intrusion Detection System**: The NRC uses the intrusion detection system to control the perimeter of the headquarter buildings.

4. **Radio Communication System**: NRC emergency-response personnel use the radio communication system to talk among one another.

5. **Building Management System**: Has two systems:

   - BMS Heating, Ventilation, & Air Conditioning (HVAC) – used to configure heating, cooling, and air ventilation in buildings 1 and 2.
   - BMS Lighting – used to control lighting in buildings 1 and 2 (intensity and degree).

6. **PIV Card Issuance Peripherals**: The NRC uses fingerprint scanners, document scanners, and photographic cameras when issuing PIV cards.

   a. Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.

   N/A.

4. What legal authority authorizes the purchase or development of this system? (*What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.*)

The systems in the ACCESS FISMA boundary are authorized through several legal authorities:

- 10 CFR parts 10, 11, 14, 25, 50, 73, 95
- 42 U.S.C. 2011 et seq.
- 42 U.S.C. 2165 and 2201(i)
- 42 U.S.C. 2165–2169, 2201, 2201a, and 2284 et seq.
- 42 U.S.C. 5801 et seq.
- 44 U.S.C. 3501, 3504, and 3541
- 44 U.S.C. 36
- 5 CFR parts 731, 732
- 5 U.S.C. 301

- E-Government Act of 2002 (Pub. L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803)
- Electronic Government Act of 2002, 44 U.S.C. 36
- Executive Order 10450, as amended
- Executive Order 10865, as amended
- Executive Order 13462, as amended by Executive Order 13516
- Executive Order 13467
- Executive Order 13526
- Executive Order 9397, as amended by Executive Order 13478
- Federal Information Security Management Act of 2002 (Pub. L. 107-296, Sec. 3544)
- Homeland Security Presidential Directive 12 (HSPD–12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- Interagency security committee standards "Physical Security Criteria for Federal Facilities," April 2010
  OMB Circular No. A–130, Revised

5. What is the purpose of the system and the data to be collected?

The purpose of the systems in the ACCESS FISMA boundary, and for the data they maintain, is to ensure the physical safety and security of personnel, property, information, infrastructure, and assets.

6. Points of Contact: (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary*.)

Project Manager	**Office/Division/Branch**	**Telephone**
Denis Brady	Office of Administration (ADM) / Division of Facilities & Security (DFS) / Security Management and Operations Branch (SMOB)	301-415-5768
Business Project Manager	**Office/Division/Branch**	**Telephone**
TBD	TBD	TBD
Technical Project Manager	**Office/Division/Branch**	**Telephone**
TBD	TBD	TBD
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Jennifer Golder	Office of Administration (ADM)	301-287-0741

ISSO	Office/Division/Branch	Telephone
Tamar Katz	Office of Administration (ADM) / Program Management, Announcements, & Editing (PMAE) / Budget & Information Technology Team (BITT)	301-287-0741
System Owner/User	**Office/Division/Branch**	**Telephone**
Jennifer Golder	Office of Administration (ADM)	301-287-0741

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ____ New System

____ Modify Existing System

__X__ Other

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

Yes.

(1) If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.

Approval Date: October 16, 2020.

Accession Number: ML20273A105.

(2) If yes, provide a summary of modifications or other changes to the existing system.

This is an annual review of the PIA prepared for an existing system.

8. Do you have an NRC system Enterprise Architecture (EA)/Inventory number?

Yes.

a. If yes, please provide the EA/Inventory number.

EA Number H0008.

b. If, no, please contact EA Service Desk to get the EA/Inventory number.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Physical Access Control System*:* Yes.

Closed-Circuit Television System: No.

Intrusion Detection System: No.

Radio Communication System: No.

Building Management System: No.

PIV Card Issuance Peripherals: No.

Although the operators of the Information Technology Infrastructure (ITI) Identity, Credential, & Access Management (ICAM) system use the PIV card issuance peripherals to collect fingerprints, facial images, and identity documents about individuals, this information is not maintained on the peripherals.

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

Physical Access Control System*:*
The PACS system has information about current and former federal employees and contractors.

Closed-Circuit Television System*:* N/A.

Intrusion Detection System: N/A.

Radio Communication System: N/A.

Building Management System: N/A.

PIV Card Issuance Peripherals: N/A.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (<u>be specific</u> – e.g. Social Security Number (SSN), Place of Birth, Name, Address)?

<u>Physical Access Control System</u>*:* The PACS system has names, facial images, badge numbers, campus, clearance level, and information about readers used with date and time.

<u>Closed-Circuit Television System</u>: None.

<u>Intrusion Detection System</u>*:* None.

<u>Radio Communication System</u>*:* None.

<u>Building Management System</u>: None.

<u>PIV Card Issuance Peripherals</u>: None.

c. Is information being collected from the subject individual? (*To the greatest extent possible, collect information about an individual directly from the individual.*)

No.

(1) If yes, what information is being collected?

N/A.

d. Will the information be collected from individuals who are not Federal employees?

Yes.

(1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?

Yes.

(a) If yes, indicate the OMB approval number:

<u>Physical Access Control System</u>. Yes.
OMB Approval Control Number: 3150-0218.

<u>Closed-Circuit Television System</u>. N/A.

<u>Intrusion Detection System</u>. N/A.

<u>Radio Communication System</u>. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

e. Is the information being collected from existing NRC files, databases, or systems?

Physical Access Control System. Yes.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

(1) If yes, identify the files/databases/systems and the information being collected.

Physical Access Control System.
The PACS system receives information from the ITI ICAM system.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

f. Is the information being collected from external sources (any source outside of the NRC)?

Physical Access Control System. No.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

(1) If yes, identify the source and what type of information is being collected?

N/A.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Physical Access Control System. The PACS system relies on the operators of the ITI ICAM system to verify the accuracy or completeness of the information that the system passes to the PACS system.

Closed-Circuit Television System. The closed-circuit television system does not collect information from individuals.

Intrusion Detection System. The intrusion detection system does not collect information from individuals.

Radio Communication System. The radio communication system does not collect information from individuals.

Building Management System. The building management system does not collect information from individuals.

PIV Card Issuance Peripherals. The PIV card issuance peripherals do not have any information which is not collected directly from the subject.

h. How will the information be collected (e.g. form, data transfer)?

Physical Access Control System. Data transfer.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

Physical Access Control System. Yes.

Closed-Circuit Television System. Yes.

Intrusion Detection System.
No. Although the intrusion detection system generates security management information (alarms) as part of its function, this information is maintained in the PACS system.

Radio Communication System. Yes.

Building Management System. No.

PIV Card Issuance Peripherals. No.

(1) If yes, identify the type of information (be specific).

Physical Access Control System. Security management information (access logs, alarms).

Closed-Circuit Television System. Security management information (camera-feeds).

Intrusion Detection System. N/A.

Radio Communication System.
Security management information (radio traffic recordings).

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Physical Access Control System.
Security management information (access logs, alarms).

Closed-Circuit Television System
Security management information (camera-feeds).

Intrusion Detection System. N/A.

Radio Communication System.
Security management information (radio traffic recordings).

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

Physical Access Control System.
The NRC uses the access control information in the PACS system to control access to the NRC campus and buildings.

The NRC emergency-response personnel use security management information (alarms) from the intrusion detection system, displayed in the PACS system, to control the perimeter of the headquarter buildings (this is not PII).

Closed-Circuit Television System.
The NRC emergency-response personnel use security management information (camera-feeds) captured by the closed-circuit TV system to monitor the headquarter campus and buildings (this is not PII).

Intrusion Detection System.
Federal protective-services emergency-response personnel use security management information (alarms) from the intrusion detection system to control the perimeter of the headquarter buildings (this is not PII).

Security management information (alarms) captured by the closed-circuit TV system is also passed to the PACS system (this is not PII).

Radio Communication System
The NRC emergency-response personnel use the radio communication system to communicate security management information (talk among one another). (this is not PII).

Building Management System.
The NRC uses the BMS Heating, Ventilation, & Air Conditioning (HVAC) to configure heating, cooling, and air ventilation in buildings 1 and 2; and the BMS Lighting system to control lighting in buildings 1 and 2.

PIV Card Issuance Peripherals.
The NRC uses the information captured by the PIV card issuance peripherals (fingerprint scanners, document scanners, and cameras) when issuing PIV cards.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Physical Access Control System. Yes.

Closed-Circuit Television System. Yes.

Intrusion Detection System. Yes.

Radio Communication System. Yes.

Building Management System. Yes.

PIV Card Issuance Peripherals. Yes.

3. Who will ensure the proper use of the data in this system?

Physical Access Control System.
The operators of the PACS system protect the information maintained in the system.

The information is protected under:

- Privacy Act Systems of Records
- SORN NRC-40, "Facility Security Access Control Records"
- SORN NRC-45, "Digital Certificate for Personal Identity Verification Records"

Closed-Circuit Television System.
The operators of the closed-circuit television system protect the security management information (camera-feeds) maintained in the system.

Intrusion Detection System.
Security management information (alarms) is transferred to the PACS system. The intrusion detection system does not retain information.

Radio Communication System.
The emergency response personnel will protect the information maintained in the system.

Building Management System.
The building management system does not preserve data information.

PIV Card Issuance Peripherals.
The administrators of the ITI ICAM system protect the privacy rights of individuals whose information they capture using the PIV card issuance peripherals. They sign a "Trusted Person Agreement."

The information is protected under:

- Privacy Act Systems of Records
- SORN NRC-45, "Digital Certificate for Personal Identity Verification Records"

4. Are the data elements described in detail and documented?

Yes.

a. If yes, what is the name of the document that contains this information and where is it located?

The ACCESS Security Categorization Report (ADAMS accession number ML19234A214, August 20, 2019) describes the data elements of the systems in the ACCESS FISMA boundary.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

Physical Access Control System. No.

Closed-Circuit Television System. No.

Intrusion Detection System. No.

Radio Communication System. No.

Building Management System. No.

PIV Card Issuance Peripherals. No.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

N/A.

b. How will aggregated data be validated for relevance and accuracy?

N/A.

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

The systems in the ACCESS FISMA boundary comply with organizational-defined computer security controls. These controls are applied to “harden” the system against unauthorized access, insider threat, compromise, or disaster.

They also comply with the change management procedures of the Office of Chief Information Officer (OCIO) to make sure only authorized work is performed on the system.

The systems comply with the policies and procedures of the OCIO computer security organization and undergoes independent continuous monitoring assessments to secure the system.

The data in the systems is restricted to application administrators in the ADM facilities security branch. These administrators have undergone rigorous background screening and are trained in their administrator duties to secure the ACCESS systems.

The system owner has also assigned primary and alternate information system security officers to the ACCESS FISMA boundary to make sure system security controls are operating as designed and intended.

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

Yes.

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Physical Access Control System. Authorized application administrators can retrieve information about an individual in the PACS system by name or by the unique identifier assigned to the person by the ITI ICAM system.

Closed-Circuit Television System. The closed-circuit television system does not maintain information about individuals.

Intrusion Detection System. The intrusion detection system does not maintain information about individuals.

Radio Communication System. The radio communication system does not maintain information about individuals.

Building Management System. The building management system does not maintain information about individuals.

PIV Card Issuance Peripherals. The PIV card issuance peripherals do not maintain information about individuals.

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes.

a. If "Yes," provide name of SORN and location in the Federal Register.

Physical Access Control System.

- Privacy Act Systems of Records
- SORN NRC-40, "Facility Security Access Control Records"
- SORN NRC-45, "Digital Certificate for Personal Identity Verification Records"

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals.

- Privacy Act Systems of Records
- SORN NRC-45, "Digital Certificate for Personal Identity Verification Records"

8. If the information system is being modified, will the SORN(s) require amendment or revision?

No.

9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

Physical Access Control System. Yes.

Closed-Circuit Television System. Yes.

Intrusion Detection System. No.

Radio Communication System. No.

Building Management System. No.

PIV Card Issuance Peripherals. No.

a. If yes, explain.

N/A.

(1) What controls will be used to prevent unauthorized monitoring?

Physical Access Control System
Logical access to the PACS system is limited to authorized users. Physical access to equipment displaying information is limited to the same authorized users.

Persons must have a need-to-know to become authorized users. They can only access information and features of the system appropriate for their job responsibility. They undergo a rigorous background screening process. Their need-to-know and access privileges are reviewed yearly.

Furthermore, data is encrypted during transport to make sure unauthorized monitoring does not occur.

Closed-Circuit Television System.
Logical access to the closed-circuit television system is limited to authorized users. Physical access to equipment is limited to the same authorized users.

Persons must have a need-to-know to become authorized users. They can only access information and features of the system appropriate for their job responsibility. They undergo a rigorous background screening process. Their need-to-know and access privileges are reviewed yearly.

Furthermore, data is encrypted during transport to make sure unauthorized monitoring does not occur.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

10. List the report(s) that will be produced from this system.

Physical Access Control System.

- Credential history reports
- Alarm history reports
- Operator history reports
- Device reports (number of card readers, number of alarm points, and so forth)

Closed-Circuit Television System. None.

Intrusion Detection System. None.

Radio Communication System. None.

Building Management System. None.

PIV Card Issuance Peripherals. None.

a. What are the reports used for?

Physical Access Control System. Investigate unauthorized activity, unauthorized access, and malfunctioning equipment, and report on compliance with federal standards.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

b. Who has access to these reports?

Physical Access Control System. Access to the reports in the PACS system is limited to authorized users. Persons must have a need-to-know to become authorized users and they can only access reports appropriate for their job responsibility. They undergo a rigorous background screening process and their need-to-know and access privileges are reviewed yearly.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. N/A.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

Physical Access Control System.

- Office of Administration, Division of Facilities and Security
- Region I, Division of Resource Management
- Region II, Division of Resource Management and Administration
- Region III, Division of Resource Management and Administration
- Region IV, Division of Resource Management and Administration
- Office of the Chief Human Capital Officer, Technical Training Center
- Office of Chief Information Officer, IT Services Development and Operations Division

Closed-Circuit Television System.

- Office of Administration, Division of Facilities and Security
- Region I, Division of Resource Management
- Region II, Division of Resource Management and Administration
- Region III, Division of Resource Management and Administration
- Region IV, Division of Resource Management and Administration
- Office of the Chief Human Capital Officer, Technical Training Center
- Office of Chief Information Officer, IT Services Development and Operations Division

Intrusion Detection System.

- Office of Administration, Division of Facilities and Security

Radio Communication System.

- Office of Administration, Division of Facilities and Security
- Region I, Division of Resource Management
- Region II, Division of Resource Management and Administration
- Region III, Division of Resource Management and Administration
- Region IV, Division of Resource Management and Administration

Building Management System.

- Office of Administration, Division of Facilities and Security

PIV Card Issuance Peripherals.

- Office of Administration, Division of Facilities and Security
- Region I, Division of Resource Management
- Region II, Division of Resource Management and Administration
- Region III, Division of Resource Management and Administration
- Region IV, Division of Resource Management and Administration

- Office of Chief Information Officer, IT Services Development and Operations Division

(1) For what purpose?

Physical Access Control System.
The Office of Administration, Division of Facilities and Security operates the PACS system.

The Region I Division of Resource Management, Region II Division of Resource Management and Administration, Region III Division of Resource Management and Administration, Region IV Division of Resource Management and Administration, and Office of the Chief Human Capital Officer Technical Training Center operate the PACS system in the respective regions.

The Office of Chief Information Officer, IT Services Development and Operations Division maintains the infrastructure on which the PACS system operates.

Closed-Circuit Television System.
The Office of Administration, Division of Facilities and Security operates the closed-circuit television system.

The Region I Division of Resource Management, Region II Division of Resource Management and Administration, Region III Division of Resource Management and Administration, Region IV Division of Resource Management and Administration, and Office of the Chief Human Capital Officer Technical Training Center operate the closed-circuit television system in the respective regions.

The Office of Chief Information Officer, IT Services Development and Operations Division maintains the infrastructure on which the closed-circuit television system operates.

Intrusion Detection System.
The Office of Administration, Division of Facilities and Security operates and maintains the intrusion detection system.

Radio Communication System.
The Office of Administration, Division of Facilities and Security operates and maintains the radio communication system.

The Region I Division of Resource Management, Region II Division of Resource Management and Administration, Region III Division of Resource Management and Administration, and Region IV Division of Resource Management and Administration operate and maintain the radio communication system in the respective regions.

Building Management System.
The Office of Administration, Division of Facilities and Security operates the building management system.

PIV Card Issuance Peripherals.
The Office of Administration, Division of Facilities and Security operates the PIV card issuance peripherals.

The Region I Division of Resource Management, Region II Division of Resource Management and Administration, Region III Division of Resource Management and Administration, and Region IV Division of Resource Management and Administration operate the PIV card issuance peripherals in the respective regions.

Office of Chief Information Officer, IT Services Development and Operations Division maintains the infrastructure on which the PIV card issuance peripherals reside.

(2) Will access be limited?

Physical Access Control System. Yes.

Closed-Circuit Television System. Yes.

Intrusion Detection System. Yes.

Radio Communication System. Yes.

Building Management System. Yes.

PIV Card Issuance Peripherals. Yes.

2. Will other NRC systems share data with or have access to the data in the system?

Physical Access Control System. Yes.

Closed-Circuit Television System. No.

Intrusion Detection System. No, not outside of the ACCESS FISMA boundary.

Radio Communication System. No.

Building Management System. No.

PIV Card Issuance Peripherals. Yes.

(1) If yes, identify the system(s).

Physical Access Control System. The ITI ICAM system passes PIV credential information to the PACS system.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals.
The PIV card issuance peripherals pass information to the ITI ICAM system.

(2) How will the data be transmitted or disclosed?

Physical Access Control System. The data is encrypted during transport.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. N/A.

PIV Card Issuance Peripherals. The data is encrypted during transport.

3. Will external agencies/organizations/public have access to the data in the system?

Physical Access Control System. No.

Closed-Circuit Television System. No.

Intrusion Detection System. No.

Radio Communication System. No.

Building Management System. Yes.

PIV Card Issuance Peripherals. No.

(1) If yes, who?

Physical Access Control System. N/A.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System. The system will be accessed remotely by the vendor, Alerton.

PIV Card Issuance Peripherals. N/A.

(2) Will access be limited?

Physical Access Control System. N/A.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System.
Yes, users will use a Virtual Private Network (VPN) connection to the system in compliance with OMB M-16-04, 30 Oct 2015.

PIV Card Issuance Peripherals. N/A.

(3) What data will be accessible and for what purpose/use?

Physical Access Control System. N/A.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System.
Configure heating, cooling, and air ventilation and control lighting.

PIV Card Issuance Peripherals. N/A.

(4) How will the data be transmitted or disclosed?

Physical Access Control System. N/A.

Closed-Circuit Television System. N/A.

Intrusion Detection System. N/A.

Radio Communication System. N/A.

Building Management System.
Through a network segmentation on a separate Citrix Virtual Desktop.

PIV Card Issuance Peripherals. N/A.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in? NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules (GRS)?

Yes.

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

See Security Records - GRS Schedule 5.6 and Facility, Equipment, Vehicle, Property, and Supply Records- GRS Schedule 5.4 in the table below which will be used for the retention of the information. If information does not fall into the items listed in GRS 5.6, then data will

need to be scheduled; therefore, NRC records personnel will need to work with staff to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

Records	Citation	Temporary/ Permanent	Disposition Instructions	Notes/Comments
Personnel Security Files and Associated Records	GRS 5.6 item 010	T	Security administrative records. Destroy when **3 years old**, but longer retention is authorized if required for business use.	BASED ON NRC SORN 39
	GRS 5.6 item 110	T	Visitor processing records. Areas requiring highest level security awareness. Destroy when **5 years old**, but longer retention is authorized if required for business use.	BASED ON NRC SORN 39
	GRS 5.6 item 111	T	Visitor processing records. All other facility security areas. Destroy when **2 years old**, but longer retention is authorized if required for business use.	BASED ON NRC SORN 39
	GRS 5.6 item 181	T	Personnel security and access clearance records. Records of people issued clearances. Destroy **5 years** after employee or contractor relationship ends, but longer retention is authorized if required for business use.	BASED ON NRC SORN 39. According to Section E.2 of PIA dated 7/26/2018, retain records for **7** years from the date personnel are deactivated (month of separation). Security management records (alarms) are retained for **7** years.

Records	Citation	Temporary/ Permanent	Disposition Instructions	Notes/Comments
Facility Security Access Control Records	GRS 5.6 item 111	T	Visitor processing records. All other facility security areas. Destroy when **2** years old, but longer retention is authorized if required for business use.	BASED ON NRC SORN 40
	GRS 5.6 item 190	T	Index to personnel security case files. Destroy when superseded or obsolete.	BASED ON NRC SORN 40
	GRS 5.6 item 090	T	Records of routine security operations. Destroy when **30 days** old, but longer retention is authorized if required for business use.	BASED ON NRC SORN 40
	GRS 5.6 item 120	T	Personal identification credentials and cards. Application and activation records. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card **6** years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.	BASED ON NRC SORN 40. According to section E.2 of PIA dated 7/26/2018, Physical access control records for a person are retained for **7** years from the date they are deactivated (month of separation). Security management records (alarms) are also retained for **7** years.
	GRS 5.6 item 170	T	Personnel security investigative reports. Personnel suitability and eligibility investigative reports. Destroy in accordance with the investigating agency instruction.	BASED ON NRC SORN 40
	GRS 5.6 item 171	T	Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority. Destroy in accordance with delegated authority agreement or memorandum of understanding.	BASED ON NRC SORN 40

Records	Citation	Temporary/ Permanent	Disposition Instructions	Notes/Comments
Electronic Credentials for Personal Identity Verification	GRS 5.6 item 120	T	Personal identification credentials and cards. Application and activation records. Destroy mandatory and optional data elements housed in the agency identity management system and printed on the identification card **6** years after terminating an employee or contractor's employment, but longer retention is authorized if required for business use.	BASED ON NRC SORN 45
	GRS 5.6 item 121	T	Cards. Destroy after expiration, confiscation, or return.	BASED ON NRC SORN 45
	GRS 5.6 item 130	T	Local facility identification and card access records. Destroy upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed **6 months** from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is required for business use.	BASED ON NRC SORN 45
Intrusion Detection (Routine)	GRS 5.6 item 090	T	Destroy when **30 days** old, but longer retention is authorized if required for business use.	According to Section C.4 of PIA, intrusion detection system does not retain information.
Intrusion Detection (Incident)	GRS 5.6 item 100	T	Destroy **3 years** after final investigation or reporting action or when **3 years old**, whichever is later, but longer retention is authorized for business use.	
Closed-Circuit Television Records	GRS 5.6 item 090	T	Records of routine security operations. Destroy when **30 days old**, but longer retention is authorized if required for business use.	See Section E.2 of PIA dated 7/26/2018, Closed-circuit Television System. Retains security management records (camera feeds) for **30 days**.
Radio Transmissions	GRS 5.6 item 090	T	Records of routine security operations. Destroy when **30 days old**, but longer retention is authorized if required for business use.	See Section E.2 of PIA dated 7/26/2018, Radio Communications System. The radio communication system retains security management records (radio traffic recordings) for a duration of a dispatch session, typically less than **24 hours**.

Records	Citation	Temporary/ Permanent	Disposition Instructions	Notes/Comments
Heating, Ventilation, & Air Conditioning (HVAC) and Lighting Records	GRS 5.4 item 010	T	Destroy when **3 years old or 3 years** after superseded, as appropriate, but longer retention is authorized if required for business use.	Administrative and operational records
	GRS 5.4 item 070	T	Destroy when **3 years old**, but longer retention is authorized if required for business use.	Inspection, maintenance and service records
	GRS 5.4 item 071	T	Destroy when **90 days old**, but longer retention is authorized if required for business use.	tracking completion of custodial and minor repair work

b. If no, please contact the RIM staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

Access to the systems in the ACCESS FISMA boundary is controlled by PIV card authentications, both to the network infrastructure and to the individual system applications. It, along with Role-Based Access Controls (RBAC), ensures only authorized persons can access data, and only data they need to conduct their job duties.

The infrastructure components of the ACCESS systems are separated through network segmentation. This architecture makes sure only authorized and authenticated devices exchange data.

The system administrators review system logs daily for unauthorized and or suspicious activities. The network administrators monitor the infrastructure for intrusions and other suspicious activities.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

All system transactions are tied to a specific, unique person's identity by strict identification and authentication protocols. The system logs all user activities.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes.

(1) If yes, where?

The criteria, procedures, controls, and responsibilities regarding access to the system are documented:

- ACCESS Security Policies and Procedures (SPP), (ADAMS accession number: ML20307A503), version 4.0, October 30, 2020
- ACCESS Consolidated System Security Plan (SSP), (ADAMS accession number: MLTBD), version 10.0, July 28, 2021

The documents are reviewed yearly.

4. Will the system be accessed or operated at more than one location (site)?

Yes.

a. If yes, how will consistent use be maintained at all sites?

All persons in the same role go through the same training, sign the same agreements, have the same access restrictions, and are subject to the same oversight independent of their physical location.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

Access to the data is strictly controlled and limited to those with an operational need to access the information.

Physical Access Control System.
- Application Users
- Application Administrators
- Server Administrators
- Database Administrators

Closed-Circuit Television System.
- Application Users
- Application Administrators

Intrusion Detection System.
- Engineers

Radio Communication System.
- Application Users
- Application Administrators
- Server Administrators

Building Management System.
- Application Users
- Application Administrators
- Server Administrators

PIV Card Issuance Peripherals.
- Application Users

6. Will a record of their access to the system be captured?

Physical Access Control System. Yes.

Closed-Circuit Television System. Yes.

Intrusion Detection System. No.

Radio Communication System. Yes.

Building Management System. Yes.

PIV Card Issuance Peripherals. No, not on the peripheral.

a. If yes, what will be collected?

Physical Access Control System. All operator transactions are logged within the system. Audit logs are generated for all transactions and security events.

Closed-Circuit Television System.
All operator transactions are logged on the workstations used to access the system. Audit logs are generated for all transactions and security events.

Intrusion Detection System. N/A.

Radio Communication System.
All operator transactions are logged within the system. Audit logs are generated for all transactions and security events.

Building Management System.
All operator transactions are logged within the system. Audit logs are generated for all transactions and security events.

PIV Card Issuance Peripherals. N/A.

7. Will contractors be involved with the design, development, or maintenance of the system?

Yes.

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (FAR) clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*

- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

All systems in the ACCESS FISMA boundary have role-based restrictions, and persons with access privileges have undergone personnel security screening. These persons undergo mandatory user awareness, role-based cybersecurity, and PII training related to their role on the information system. Data is safeguarded in transmission using encryption and access controlled private virtual networks. The information system security officers receive audit logs daily.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?

FY14 ACCESS Authority to Operate (ATO) – April 17, 2014, ML14070A318.

b. If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?

N/A.

c. If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.

N/A.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMSD/CSB Staff)

System Name: Automated Access Control and Computer Enhance Security System (ACCESS)

Submitting Office: OCIO

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:

This system is covered under NRC Privacy Act systems of records NRC-39, "Personnel Security Files and Associated Records," NRC-40, "Facility Security Access Controls Records," and NRC-45, "Digital Certificates for Personal Identity Verification Records.

Reviewer's Name	Title
Signed by Hardy, Sally on 09/28/21	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

____ No OMB clearance is needed.

____ OMB clearance is needed.

__X__ Currently has OMB Clearance. Clearance No. Currently has OMB Clearance. Clearance No. 3150-0046 (10 CFR Part 25) and 3150-0218 (NRC Form 850)

Comments:

Reviewer's Name	Title
Signed by Cullison, David on 09/23/21	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

____ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 09/24/21	Sr. Program Analyst, Electronic Records Manager

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

____ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

 Signed by Nalabandian, Garo on 10/05/21

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: Jennifer Golder, Office of Administration (ADM)	
Name of System: Automated Access Control and Computer Enhanced Security System (ACCESS)	
Date CSB received PIA for review: September 3, 2021	**Date CSB completed PIA review:** September 28, 2021
Noted Issues: Note there is an unauthorized portion of the ACCESS FISMA system that is limited to one subsystem. This subsystem is due to be authorized during fiscal year 2022. The other parts of the system are in an ongoing authorization status.	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Nalabandian, Garo on 10/05/21
Copies of this PIA will be provided to: *Thomas G. Ashley, Jr.* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Jonathan R. Feibus* *Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	